PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-290708
(43)Date of publication of application : 19.10.2001

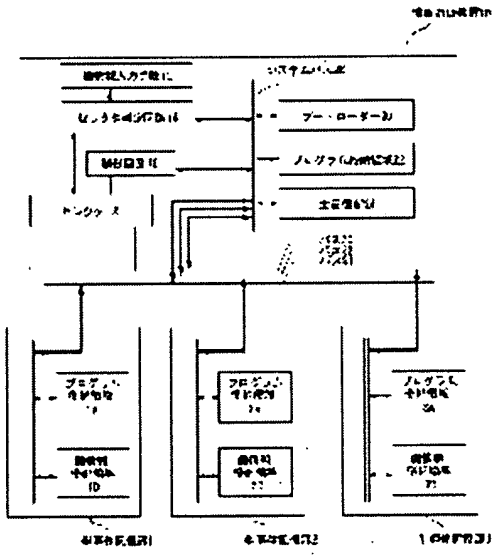
(51)Int.Cl. G06F 12/14
G06F 9/06

(21)Application number : 2000-104283
(22)Date of filing : 06.04.2000

(71)Applicant : NEC CORP
(72)Inventor : IIZUKA HIROSHI

(54) INFORMATION PROCESSOR AND PRIVATE INFORMATION SECURITY METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an information processor and a private information security method capable of preventing a program or data managed by an individual from being used or quoted by others.
SOLUTION: This processor has a plurality of freely attachable and detachable semiconductor storing parts 1, 2 and 3 provided with program storage areas 1A, 2A and 3A and key information storage areas 1B, 2B and 3B, a selector 18 selecting and connecting any of the parts 1, 2 and 3 to a system bus 26, a key information inputting means 12 for being able to input key information from the outside and a selector decision circuit 14 for deciding which to be selected among the parts 1, 2 and 3 with the selector 18, and the selector decision circuit 14 makes the selector 18 select a coinciding semiconductor storing part 1, 2 or 3 obtained by comparing the pieces of key information of the areas 1B, 2B and 3B with the key information from the means 12.



LEGAL STATUS

[Date of request for examination]	09.03.2001
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3551889
[Date of registration]	14.05.2004
[Number of appeal against examiner's decision of rejection]	

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] It has a program storage area and a key information storing field. Two or more semi-conductor storage sections which can be detached and attached freely, The selector which some choose one among said two or more semi-conductor storage sections, and is connected to a system bus, It has the selector judging circuit which judges it to be the key information input means which enables the input of key information from the exterior said which semi-conductor storage section to be chosen by said selector. Said selector judging circuit The information processor characterized by having the function to which said semi-conductor storage section is made to choose it as said selector although the key information inputted from the key information included in said key information storing field of said semi-conductor storage section and said key information input means was compared and it was in agreement.
[Claim 2] Each of two or more of said semi-conductor storage sections is connected to a predetermined bus, and said bus is alternatively connected to said system bus by said selector. A boot loader, a program storage area, a primary storage, the control circuit containing CPU, and said selector judging circuit are connected to said system bus, respectively. Said key information input means Have the function which acquires key information from the exterior, connect with said selector judging circuit, and key information is transmitted to said selector judging circuit. Said selector judging circuit is an information processor according to claim 1 characterized by being constituted so that it may connect with said selector, either of said buses may be connected to said system bus and directions may be taken out to said selector.
[Claim 3] Said selector is an information processor according to claim 2 characterized by having a means to acquire each key information on said two or more semi-conductor storage sections, and to transmit to said selector judging circuit.
[Claim 4] An information processor given in claim 1 characterized by constituting said semi-conductor storage section with the IC card thru/or any 1 term of 3.
[Claim 5] The information processor according to claim 4 characterized by performing the program of individual possession and processing using private data by setting said IC card in equipment and giving key information from outside.
[Claim 6] It has a program storage area and a key information storing field. Two or more semi-conductor storage sections which can be detached and attached freely, The selector which some choose one among said two or more semi-conductor storage sections, and is connected to a system bus, It has the selector judging circuit which judges it to be the key information input means which enables the input of key information from the exterior said which semi-conductor storage section to be chosen by said selector. Said selector judging circuit In the information processor which has the function to which said semi-conductor storage section is made to choose it as said selector although the key information inputted from the key information included in said key information storing field of said semi-conductor storage section and said key information input means was compared and it was in agreement The process which memorizes specific key information which is different, respectively to said each key

information storing field of two or more of said semi-conductor storage sections, The process said selector recognizes said key information to be through a bus, and the process which collects each key information that said selector judging circuit gives a demand to said selector, and is memorized by said semi-conductor storage section, The process at which said key information input means acquires key information from the exterior, and the process which sends the key information which came to hand with said key information input means to said selector judging circuit, When said selector judging circuit has recognized it as the key information on said semi-conductor storage section and the key information acquired from said key information input means having been in agreement, while controlling said selector and connecting said bus to said system bus It notifies that said selector connected the bus concerned to said system bus to said control circuit. The process at which said control circuit starts a boot loader and transmits the program storage area of said semi-conductor storage section to a program to said program storage area linked to said system bus based on the notice from said selector, The process which performs the transmitted program concerned using CPU of said control circuit, Based on the key information newly acquired from said key information input means, said selector judging circuit is the personal-feelings news security approach characterized by having the process which interrupts said control circuit through said system bus, and stops the program under activation.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to a personal-feelings news management technique, and relates to the information processor and the personal-feelings news security approach of preventing others' using or quoting the program or data which each people use a private program or data independently, and manages them individually based on key information in the environment which can be touched by two or more men especially with one equipment.
[0002]
[Description of the Prior Art] In recent years, in the note type personal computer etc., as external storage, it has a PCMCIA interface etc. and the flash memory card connected with the body of a personal computer removable is used.
[0003] However, the data memorized by flash memory card sampled the flash memory card from the body of a personal computer, connected with other computers etc., and when accessing, they were able to be easily read regardless of those who access. For this reason, flash memory card did not fit the data storage for confidentiality.
[0004] As a conventional technique aiming at solving such a trouble, the thing of a publication is in JP,11-265318,A, for example. The conventional technique is a thing aiming at offering the mutual recognition system and the mutual recognition approach of attesting those who perform access to the data memorized by the removable store. Namely, a storage means, It is constituted by the access means. An access means A means to create the 1st authentication data based on the password supplied by actuation of an operator, The 1st digest creation means which creates the 1st digest showing a means to create a delivery key and to supply a storage means, and the thing which changed the 1st authentication data so that inverse transformation could not be performed substantially, The 2nd digest showing what changed the 1st authentication data so that inverse transformation could not be performed substantially is created, and it has the 2nd digest creation means supplied to a storage means. A storage means A data storage means equipped with the storage region for storing data, and a means to memorize the 2nd enciphered authentication data, A means to decrypt the 2nd enciphered authentication data using the delivery key supplied from the access means, The 3rd digest creation means which creates the 3rd digest showing what changed the 2nd authentication data so that inverse transformation could not be performed substantially, and is supplied to an access means, The 4th digest creation means which creates the 4th digest showing what changed the 2nd authentication data so that inverse transformation could not be performed substantially, When it was distinguished and shown whether the 2nd digest is acquired from an access means and the 2nd and 4th digests show the same authentication data substantially and it is distinguished, Storing to the data storage field supplied from the access means according to directions of an access means, It has a means to perform supply for the access means of the data acquired from acquisition of the data from a storage region, and a storage region. An access means When it was distinguished and shown whether the 3rd digest is acquired from a storage means and the 1st and 3rd digests show the same authentication data substantially and it is distinguished, The storage means is

equipped with the means which supplies the data to the directions which require acquisition of the data from a storage region, the directions which require storing of the data to a storage region, and a storage means.

[0005] According to such a mutual recognition system, after checking that a storage means and an access means have the authentication data memorized by the storage means and the substantially same authentication data made from the password supplied to the access means, access to the storage region of a data storage means is permitted to a user etc. Therefore, if it is made not to open a password to persons other than a user, authentication of those who perform access to data will be performed.

[0006] An access means creates a user key based on a password, enciphers a user key using a delivery key, and creates an encryption user key. It has a means to supply an encryption user key to a storage means. A storage means A means by which access from an access means has an impossible storage region substantially, and memorizes a system key, the 2nd enciphered authentication data, and the enciphered proper key all over a storage region, A means to decrypt the encryption user key supplied from the access means using a delivery key, A proper key decryption means to decrypt the enciphered proper key using a system key and the decrypted user key, The 1st enciphered authentication data may be decrypted using the decrypted proper key, and you may have an authentication data decryption means to create the 2nd authentication data. Thereby, since the secrecy nature of the data which the secrecy nature of the 2nd authentication data increases, and are used for a decryption of the 2nd authentication data also increases, risk of access to a storage means being accidentally permitted by unjust actuation etc. decreases.

[0007] When a storage means supplies the data of the object which an access means performs the directions which require storing of the data to a storage region, and stores in a storage region, When the directions whose means to encipher using the decrypted proper key and to store the supplied data in a storage region and access means require acquisition of the data stored in the storage region are performed, The data enciphered may be acquired from a storage region, may be decrypted using the decrypted proper key, and you may have a means to supply an access means. Thereby, the data stored in the storage region of a data storage means are stored after having been enciphered by the proper key. For this reason, the contents of data are not revealed unless those who performed unjust access know a proper key, even if it receives access with an unjust storage region, for example. Therefore, the secrecy nature of data increases further.

[0008] The data and the decrypted proper key generated in order that a proper key decryption means may decrypt the enciphered proper key You may be a thing equipped with a means to prevent substantially that an access means is supplied. Moreover, an authentication data decryption means The data and the 2nd authentication data which are generated in order to decrypt the 1st enciphered authentication data may be equipped with a means to prevent substantially that an access means is supplied. Since the data generated by this in the process which restores a proper key and authentication data are also kept secret, the risk of leakage, a proper key, and authentication data being counted for data backward outside also decreases.

[0009] A means for an access means to acquire the 1st delivery key information from a means to generate the 1st random number, and a storage means, and to create the 1st delivery key based on the 1st delivery key information and 1st random number, The 2nd random number is acquired from a storage means, the 2nd delivery key information is created based on the 2nd random number and 1st random number, and it has a means to supply the 2nd delivery key information to a storage means. A storage means A means to generate the 2nd random number and 3rd random number, and a means to create the 1st delivery key information based on the 2nd and 3rd random numbers, and to supply the 1st delivery key information and 2nd random number to an access means, Based on the 2nd delivery key information supplied from the 3rd random number and access means, you may have the 1st delivery key and a means to create the 2nd same delivery key substantially. Thereby, since a delivery key is also sent to a storage means from an access means, with secrecy nature maintained, a delivery key is acquired unjustly and the risk of the data exchanged between an access means and a storage means being decrypted unjustly also decreases.

[0010] The 1st thru/or the 4th digest are equipped with the means which for example, an access means generates the 4th random number, and supplies to a storage means. The 1st digest creation means The 1st authentication data, It has a means to create the 1st digest by [which make the 4th random number a variable] on the other hand calculating the tropism value of a function. The 2nd digest creation means The 1st authentication data, It has a means to create the 2nd digest by [which make the 3rd random number a variable] on the other hand calculating the tropism value of a function. The 3rd digest creation means The 2nd authentication data, It has a means to create the 3rd digest by [which make the 4th random number a variable] on the other hand calculating the tropism value of a function. The 4th digest creation means The 2nd authentication data, It is generated by having a means to create the 4th digest by [which make the 3rd random number a variable] on the other hand calculating the tropism value of a function.

[0011] An access means the identification information which is supplied according to actuation of an operator and which identifies an operator The signature information which changes so that inverse transformation cannot be performed substantially, and specifies an operator is created, and it has a means to supply signature information to a storage means. A storage means When it did not distinguish and memorize whether signature information would be memorized in a storage region and distinguished from a means to acquire the signature information supplied from the access means, When the signature information supplied from the access means was memorized to the storage region, and it memorized and is distinguished, When the signature information memorized and the signature information supplied from the access means did not distinguish and show whether the same operator would be shown substantially and it is distinguished, you may have a means to refuse following the directions which an access means performs. When there are those who already accessed the storage region of a data storage means by this, since it is prevented substantially that persons other than the person access a storage region, risk of the data in a storage region being acquired by other persons decreases.

[0012]

[Problem(s) to be Solved by the Invention] However, since it was difficult for each people to use a private program or data independently based on key information in an environment with two or more men able to touch the conventional technique with one equipment, there was a trouble that it could not prevent others' using or quoting the program or data managed individually.

[0013] this invention be make in view of this trouble , and the place make into the purpose be in the point of offer the information processor and the personal feelings news security approach of prevent others use or quote the program or the data which each people use independently a private program or data based on key information , and manage them individually with one equipment in the environment which can be touch by two or more men .

[0014]

[Means for Solving the Problem] The summary of invention according to claim 1 is equipped with a program storage area and a key information storing field. Two or more semi-conductor storage sections which can be detached and attached freely, The selector which some choose one among said two or more semi-conductor storage sections, and is connected to a system bus, It has the selector judging circuit which judges it to be the key information input means which enables the input of key information from the exterior said which semi-conductor storage section to be chosen by said selector. Said selector judging circuit Although the key information inputted from the key information included in said key information storing field of said semi-conductor storage section and said key information input means was compared and it was in agreement, it consists in the information processor characterized by having the function to which said semi-conductor storage section is made to choose it as said selector. Moreover, it connects with a bus predetermined [summary / of invention according to claim 2] in each of two or more of said semi-conductor storage sections. Said bus is alternatively connected to said system bus by said selector. A boot loader, a program storage area, a primary storage, the control circuit containing CPU, and said selector judging circuit are connected to said system bus, respectively. Said key information input means Have the function which acquires key information from the exterior, connect with said selector judging circuit, and key information is transmitted to said selector judging

circuit. Said selector judging circuit consists in the information processor according to claim 1 characterized by being constituted so that it may connect with said selector, either of said buses may be connected to said system bus and directions may be taken out to said selector. Moreover, the summary of invention according to claim 3 consists in the information processor according to claim 2 characterized by said selector having a means to acquire each key information on said two or more semi-conductor storage sections, and to transmit to said selector judging circuit. Moreover, the summary of invention according to claim 4 consists in an information processor given in claim 1 characterized by constituting said semi-conductor storage section with the IC card thru/or any 1 term of 3. Moreover, by setting said IC card in equipment and giving key information from outside, the summary of invention according to claim 5 performs the program of individual possession, and consists in the information processor according to claim 4 characterized by processing using private data. The summary of invention according to claim 6 is equipped with a program storage area and a key information storing field. Moreover, two or more semi-conductor storage sections which can be detached and attached freely, The selector which some choose one among said two or more semi-conductor storage sections, and is connected to a system bus, It has the selector judging circuit which judges it to be the key information input means which enables the input of key information from the exterior said which semi-conductor storage section to be chosen by said selector. Said selector judging circuit In the information processor which has the function to which said semi-conductor storage section is made to choose it as said selector although the key information inputted from the key information included in said key information storing field of said semi-conductor storage section and said key information input means was compared and it was in agreement The process which memorizes specific key information which is different, respectively to said each key information storing field of two or more of said semi-conductor storage sections, The process said selector recognizes said key information to be through a bus, and the process which collects each key information that said selector judging circuit gives a demand to said selector, and is memorized by said semi-conductor storage section, The process at which said key information input means acquires key information from the exterior, and the process which sends the key information which came to hand with said key information input means to said selector judging circuit, When said selector judging circuit has recognized it as the key information on said semi-conductor storage section and the key information acquired from said key information input means having been in agreement, while controlling said selector and connecting said bus to said system bus It notifies that said selector connected the bus concerned to said system bus to said control circuit. The process at which said control circuit starts a boot loader and transmits the program storage area of said semi-conductor storage section to a program to said program storage area linked to said system bus based on the notice from said selector, The process which performs the transmitted program concerned using CPU of said control circuit, Based on the key information newly acquired from said key information input means, said selector judging circuit interrupts said control circuit through said system bus, and consists in the personal-feelings news security approach characterized by having the process which stops the program under activation.

[0015]

[Embodiment of the Invention] (Gestalt of the 1st operation) Drawing 1 is a functional block diagram for explaining the information processor 10 concerning the gestalt of 1 operation of this invention. drawing 1 -- setting -- 1, 2, and 3 -- the semi-conductor storage section, and 1A, 2A and 3A -- a program storage area, 1B, 2B, and 3B -- a key information storing field and 10 -- an information processor and 12 -- a key information input means and 14 -- a selector judging circuit and 16 -- a control circuit and 18 -- in a selector and 20, a primary storage and 26 show a system bus and, as for a boot loader and 22, 31, 32, and 33 show the bus, as for a program storage area and 24.

[0016] The information processor 10 of the gestalt of this operation is equipped with program storage area 1A and key information storing field 1B. The semi-conductor storage section 1 which can be detached and attached freely, It has program storage area 2A and key information storing field 2B. Two or more semi-conductor storage sections 2 which can be detached and attached freely, It has program storage area 3A and key information storing field 3B. Two or more semi-conductor storage sections 3

which can be detached and attached freely, The selector 18 which some choose one among each semi-conductor storage sections 1, 2, and 3, and is connected to a system bus 26, It has the selector judging circuit 14 which judges it to be the key information input means 12 which enables the input of key information from the exterior which semi-conductor storage sections 1, 2, and 3 to be chosen by the selector 18. The selector judging circuit 14 has the description at the point of having the function to which the semi-conductor storage sections 1, 2, and 3 which compared the key information inputted from the key information and the key information input means 12 of going into key information storing field 1B of the semi-conductor storage sections 1, 2, and 3, 2B, and 3B, and were in agreement are made choosing it as a selector 18.

[0017] The semi-conductor storage sections 1, 2, and 3 are connected to buses 31, 32, and 33, respectively. Buses 31, 32, and 33 are alternatively connected to a system bus 26 by the selector 18.

[0018] A boot loader 20, the program storage area 22, the primary storage 24, the control circuit 16 containing CPU, and the selector judging circuit 14 are connected to the system bus 26, respectively.

[0019] It has the function which acquires key information from the exterior, and connects with the selector judging circuit 14, and the key information input means 12 transmits key information to the selector judging circuit 14.

[0020] The selector judging circuit 14 takes out directions to a selector 18 so that it may connect with a selector 18 and either of the buses 31, 32, and 33 may be connected to a system bus 26.

[0021] Moreover, a selector 18 has a means to acquire the key information on the semi-conductor storage sections 1, 2, and 3, and to transmit to the selector judging circuit 14.

[0022] Next, actuation (the personal-feelings news security approach) of an information processor 10 is explained. If drawing 1 is referred to, specific key information different, respectively is memorized by key information storing field 1B of two or more semi-conductor storage sections 1, 2, and 3, 2B, and 3B in the gestalt of this operation.

[0023] A selector 18 can recognize this key information through buses 31, 32, and 33. The selector judging circuit 14 collects each key information which gives a demand to a selector 18 and is memorized by the semi-conductor storage sections 1, 2, and 3.

[0024] The key information input means 12 has a means to acquire key information from the exterior. For example, a user enters a password from a keyboard or inputting fingerprint information from a scanner is also included. the concept of a key -- palm-print information and iris information -- in addition to this, although it is various, the password is assumed as key information here. That is, a key may be read as a password. The key information which came to hand with the key information input means 12 is sent to the selector judging circuit 14.

[0025] Here, when the selector judging circuit 14 has recognized it as the key information on the semi-conductor storage section 1 and the key information acquired from the key information input means 12 having been in agreement, a selector 18 is controlled and a bus 31 is connected to a system bus 26. It notifies that the selector 18 connected the bus 31 to the system bus 26 to a control circuit 16. If, as for this notice, either is connected to the system bus 26 not only among the bus 31 but among the buses 32 and 33, a selector 18 will notify to a control circuit 16.

[0026] Based on the notice from a selector 18, a control circuit 16 starts a boot loader 20, and transmits a program to the program storage area 22 linked to a system bus 26 from program storage area 1A of the semi-conductor storage section 1. And the transmitted program is performed using CPU of a control circuit 16.

[0027] Based on the key information newly acquired from the key information input means 12, the selector judging circuit 14 interrupts a control circuit 16 through a system bus 26, and stops the program under activation.

[0028] In addition, although the semi-conductor storage sections 1, 2, and 3 showed three examples with the gestalt of this operation, it is easy to consider the escape from one to n (natural number) individual of finite, without being limited to especially this.

[0029] Since the gestalt of this operation is constituted as mentioned above, the effectiveness hung up over below is done so. First, since the 1st effectiveness can make key information able to input and can

perform the program of the semi-conductor storage sections 1, 2, and 3 corresponding to it, it is being able to make it operate using the program and data which those [each] who hold a key need.
[0030] moreover -- from [that other men cannot be made to perform the 2nd effectiveness] -- mistaking -- ** -- it is being able to forbid using a program and data by intentionally [clear].
[0031] Moreover, the 3rd effectiveness is being able to choose a required program alternatively by two or more semi-conductor storage sections 1, 2, and 3 being connectable. For example, when it is assumed that this information processor 10 is used as a TV game, the effectiveness that a user can use a required program (game) now, choosing is done so.
[0032] And the 4th effectiveness is that modification or an escape of a program can perform easily by attaching the semi-conductor storage sections 1, 2, and 3, and supposing that it is dismountable. For example, when the data of a digital camera and musical digital data are put into the semi-conductor storage sections 1, 2, and 3 at a program and coincidence, the effectiveness of coming to be able to perform exchange of data easily if needed is done so.
[0033] (gestalt of the 2nd operation) when the semi-conductor storage sections 1 , 2 , and 3 be constitute by the IC card , set in an information processor 10 and give key information from outside , the gestalt of this operation perform the program of individual possession , and have the description at the point of process using private data .
[0034] In addition, it is clear that this invention is not limited to the gestalt of each above-mentioned implementation, but the gestalt of each operation may be suitably changed within the limits of the technical thought of this invention. Moreover, the number of the above-mentioned configuration members, a location, a configuration, etc. are not limited to the gestalt of the above-mentioned implementation, but when carrying out this invention, they can be made into a suitable number, a location, a configuration, etc. Moreover, in each drawing, the same sign is given to the same component.

[0035]
[Effect of the Invention] Since this invention is constituted as mentioned above, the effectiveness hung up over below is done so. First, since the 1st effectiveness can make key information able to input and can perform the program of the semi-conductor storage section corresponding to it, it is being able to make it operate using the program and data which those [each] who hold a key need.
[0036] moreover -- from [that other men cannot be made to perform the 2nd effectiveness] -- mistaking -- ** -- it is being able to forbid using a program and data by intentionally [clear].
[0037] Moreover, the 3rd effectiveness is being able to choose a required program alternatively by two or more semi-conductor storage sections being connectable. For example, when it is assumed that this information processor is used as a TV game, the effectiveness that a user can use a required program (game) now, choosing is done so.
[0038] And the 4th effectiveness is that modification or an escape of a program can perform easily by attaching the semi-conductor storage section and supposing that it is dismountable. For example, when the data of a digital camera and musical digital data are put into the semi-conductor storage section at a program and coincidence, the effectiveness of coming to be able to perform exchange of data easily if needed is done so.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is a functional block diagram for explaining the information processor concerning the gestalt of 1 operation of this invention.
[Description of Notations]
1, 2, 3 -- Semi-conductor storage section
1A, 2A, 3A -- Program storage area
1B, 2B, 3B -- Key information storing field
10 -- Information processor
12 -- Key information input means
14 -- Selector judging circuit
16 -- Control circuit
18 -- Selector
20 -- Boot loader
22 -- Program storage area
24 -- Primary storage
26 -- System bus
31, 32, 33 -- Bus

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－290708
（P2001－290708A）
(43)公開日　平成13年10月19日(2001.10.19)

(51)Int.Cl.'	識別記号	FI	テーマコード'(参考)
G06F 12/14	320	G06F 12/14	320C 5B017
9/06	550	9/06	550J 5B076

審査請求 有　請求項の数6 OL （全 7 頁）

(21)出願番号　特願2000－104283(P2000－104283)

(22)出願日　平成12年4月6日(2000.4.6)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目7番1号

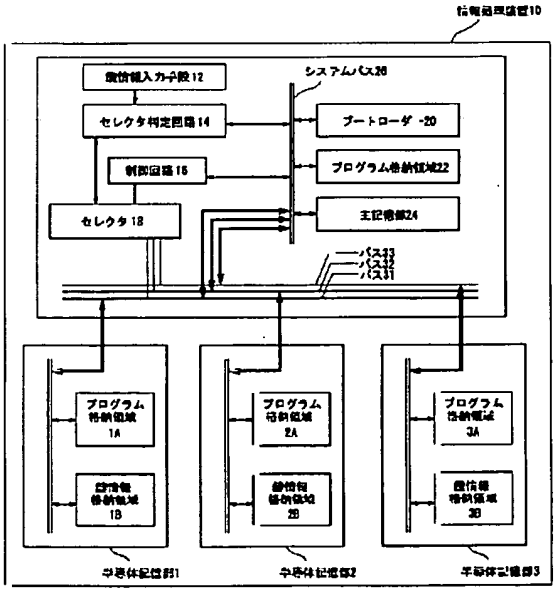
(72)発明者　飯塚　浩
東京都港区芝五丁目7番1号　日本電気株式会社内

(74)代理人　10009/113
弁理士　堀　城之

Fターム(参考)　5B017 AA07 BA05 BB03 CA14 CA15
5B076 FB06

(54)【発明の名称】　情報処理装置および私情報セキュリティ方法

(57)【要約】
【課題】　本発明は、個人で管理するプログラムあるいはデータを他人に使用あるいは引用されることを防ぐことができる情報処理装置および私情報セキュリティ方法を提供することを課題とする。
【解決手段】　プログラム格納領域１Ａ，２Ａ，３Ａと鍵情報格納領域１Ｂ，２Ｂ，３Ｂを備え着脱自在な複数の半導体記憶部１，２，３と、半導体記憶部１，２，３のいずれかを選択してシステムバス２６に接続するセレクタ１８と、外部より鍵情報を入力可能とする鍵情報入力手段１２と、セレクタ１８でどの半導体記憶部１，２，３を選択するかを判断するセレクタ判定回路１４を有し、セレクタ判定回路１４は、鍵情報格納領域１Ｂ，２Ｂ，３Ｂの鍵情報と鍵情報入力手段１２からの鍵情報を比較して一致した半導体記憶部１，２，３をセレクタ１８に選択させる。



【特許請求の範囲】
【請求項１】　プログラム格納領域と鍵情報格納領域を備え着脱自在な複数の半導体記憶部と、
前記複数の半導体記憶部のうちでどれか一つを選択してシステムバスに接続するセレクタと、
外部より鍵情報を入力可能とする鍵情報入力手段と、
前記セレクタでどの前記半導体記憶部を選択するかの判断を行うセレクタ判定回路を有し、
前記セレクタ判定回路は、前記半導体記憶部の前記鍵情報格納領域に入っている鍵情報と前記鍵情報入力手段から入力された鍵情報とを比較して一致したものの前記半導体記憶部を前記セレクタに選択させる機能を有することを特徴とする情報処理装置。
【請求項２】　前記複数の半導体記憶部のそれぞれは所定のバスに接続され、
前記バスは前記セレクタによって選択的に前記システムバスに接続され、
前記システムバスにはブートローダー、プログラム格納領域、主記憶部、ＣＰＵを含む制御回路、前記セレクタ判定回路がそれぞれ接続され、
前記鍵情報入力手段は、外部から鍵情報を取得する機能を有し、前記セレクタ判定回路に接続し鍵情報を前記セレクタ判定回路に伝達し、
前記セレクタ判定回路は前記セレクタに接続し前記バスのいずれかを前記システムバスに接続するよう前記セレクタに指示を出すように構成されていることを特徴とする請求項１に記載の情報処理装置。
【請求項３】　前記セレクタは前記複数の半導体記憶部のそれぞれの鍵情報を取得し前記セレクタ判定回路に伝達する手段を有することを特徴とする請求項２に記載の情報処理装置。
【請求項４】　前記半導体記憶部がＩＣカードにより構成されていることを特徴とする請求項１乃至３のいずれか一項に記載の情報処理装置。
【請求項５】　前記ＩＣカードを装置にセットして鍵情報を外から与えることにより、個人所有のプログラムを実行させ、プライベートなデータを使って処理を行うことを特徴とする請求項４に記載の情報処理装置。
【請求項６】　プログラム格納領域と鍵情報格納領域を備え着脱自在な複数の半導体記憶部と、前記複数の半導体記憶部のうちでどれか一つを選択してシステムバスに接続するセレクタと、外部より鍵情報を入力可能とする鍵情報入力手段と、前記セレクタでどの前記半導体記憶部を選択するかの判断を行うセレクタ判定回路を有し、
前記セレクタ判定回路は、前記半導体記憶部の前記鍵情報格納領域に入っている鍵情報と前記鍵情報入力手段から入力された鍵情報とを比較して一致したものの前記半導体記憶部を前記セレクタに選択させる機能を有する情報処理装置において、
前記複数の半導体記憶部のそれぞれの前記鍵情報格納領域にそれぞれ異なる特定の鍵情報を記憶する工程と、
前記セレクタが前記鍵情報をバスを通して認識する工程と、
前記セレクタ判定回路が前記セレクタに要求を出して前記半導体記憶部に記憶されている各鍵情報を収集する工程と、
前記鍵情報入力手段が外部から鍵情報を取得する工程と、
前記鍵情報入力手段で入手した鍵情報を前記セレクタ判定回路に送る工程と、
前記半導体記憶部の鍵情報と前記鍵情報入力手段から取得した鍵情報が一致したと前記セレクタ判定回路が認識した場合に、前記セレクタを制御して前記バスを前記システムバスに接続するとともに、前記セレクタが当該バスを前記システムバスに接続したことを前記制御回路に通知し、
前記セレクタからの通知を基に前記制御回路が、ブートローダーを起動して前記半導体記憶部のプログラム格納領域からプログラムを、前記システムバスに接続している前記プログラム格納領域に転送する工程と、
当該転送されたプログラムを前記制御回路のＣＰＵを用いて実行する工程と、
新たに前記鍵情報入力手段から取得した鍵情報を基に、前記セレクタ判定回路は前記システムバスを通して前記制御回路に割り込み、実行中のプログラムを停止する工程を有することを特徴とする私情報セキュリティ方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、私情報管理技術に係り、特に一台の装置で複数の人がさわることが可能な環境でプライベートなプログラムあるいはデータを鍵情報を基にして各個人が独立して使用し、個人で管理するプログラムあるいはデータを他人に使用あるいは引用されることを防ぐことができる情報処理装置および私情報セキュリティ方法に関する。
【０００２】
【従来の技術】近年、ノート型パーソナルコンピュータ等において、外部記憶装置として、ＰＣＭＣＩＡインターフェース等を備え、パーソナルコンピュータ本体と着脱可能に接続されるフラッシュメモリカードが用いられている。
【０００３】しかし、フラッシュメモリカードに記憶されたデータは、そのフラッシュメモリカードをパーソナルコンピュータ本体から抜き取って他のコンピュータ等に接続し、アクセスすれば、アクセスする者を問わず容易に読み取ることができた。このため、フラッシュメモリカードは、守秘対象のデータの記憶には適さなかった。
【０００４】このような問題点を解決することを目的とする従来技術としては、例えば、特開平１１－２６５３

１８号公報に記載のものがある。すなわち、従来技術は、着脱可能な記憶装置に記憶されたデータへのアクセスを行う者を認証することができる相互認証システムおよび相互認証方法を提供することを目的とするものであって、記憶手段と、アクセス手段とにより構成され、アクセス手段は、操作者の操作により供給されるパスワードに基づいて第１の認証データを作成する手段と、配送キーを作成して記憶手段に供給する手段と、第１の認証データを実質的に逆変換を行えないように変換したものを表す第１のダイジェストを作成する第１のダイジェスト作成手段と、第１の認証データを実質的に逆変換を行えないように変換したものを表す第２のダイジェストを作成し、記憶手段に供給する第２のダイジェスト作成手段とを備え、記憶手段は、データを格納するための記憶領域を備えるデータ格納手段と、暗号化された第２の認証データを記憶する手段と、アクセス手段より供給された配送キーを用いて、暗号化された第２の認証データを復号化する手段と、第２の認証データを実質的に逆変換を行えないように変換したものを表す第３のダイジェストを作成し、アクセス手段に供給する第３のダイジェスト作成手段と、第２の認証データを実質的に逆変換を行えないように変換したものを表す第４のダイジェストを作成する第４のダイジェスト作成手段と、アクセス手段より第２のダイジェストを取得して、第２および第４のダイジェストが実質的に同一の認証データを示すか否かを判別し、示すと判別されたとき、アクセス手段の指示に従って、アクセス手段から供給されたデータの記憶領域への格納、記憶領域からのデータの取得および記憶領域から取得したデータのアクセス手段への供給を行う手段とを備え、アクセス手段は、記憶手段より第３のダイジェストを取得して、第１および第３のダイジェストが実質的に同一の認証データを示すか否かを判別し、示すと判別されたとき、記憶手段に記憶領域からのデータの取得を要求する指示、記憶領域へのデータの格納を要求する指示および記憶手段へのデータの供給を行う手段を備えている。

【０００５】このような相互認証システムによれば、記憶手段とアクセス手段は、記憶手段に記憶された認証データと、アクセス手段に供給されたパスワードから作られる認証データとが実質的に同一のものであることを確認してから、データ格納手段の記憶領域へのアクセスをユーザ等に許可する。従って、パスワードをユーザ以外の者に公開しないようにすれば、データへのアクセスを行う者の認証が行われる。

【０００６】アクセス手段は、パスワードに基づいてユーザキーを作成して、ユーザキーを配送キーを用いて暗号化して暗号化ユーザキーを作成し、暗号化ユーザキーを記憶手段に供給する手段を備え、記憶手段は、アクセス手段からのアクセスが実質的に不可能な記憶領域を有し、記憶領域中に、システムキー、暗号化された第２の認証データおよび暗号化された固有キーを記憶する手段と、配送キーを用いて、アクセス手段より供給された暗号化ユーザキーを復号化する手段と、暗号化された固有キーを、システムキーおよび復号化されたユーザキーを用いて復号化する固有キー復号化手段と、暗号化された第１の認証データを、復号化された固有キーを用いて復号化し、第２の認証データを作成する認証データ復号化手段とを備えるものであってもよい。これにより、第２の認証データの秘匿性は高まり、また、第２の認証データの復号化のために用いられるデータの秘匿性も高まるので、不正な操作等により記憶手段へのアクセスが誤って許可される危険が減少する。

【０００７】記憶手段は、アクセス手段が、記憶領域へのデータの格納を要求する指示を行い、かつ、記憶領域に格納する対象のデータの供給を行ったとき、供給されたデータを、復号化された固有キーを用いて暗号化して、記憶領域に格納する手段と、アクセス手段が、記憶領域に格納されているデータの取得を要求する指示を行ったとき、暗号化されているデータを記憶領域より取得し、復号化された固有キーを用いて復号化して、アクセス手段に供給する手段とを備えるものであってもよい。これにより、データ格納手段の記憶領域に格納されるデータは固有キーにより暗号化された状態で格納される。このため、例えば記憶領域が不正なアクセスを受けても、不正なアクセスを行った者が固有キーを知らない限り、データの内容が漏洩することはない。従って、データの秘匿性は更に高まる。

【０００８】固有キー復号化手段は、暗号化された固有キーを復号化するために生成するデータおよび復号化された固有キーが、アクセス手段に供給されることを実質的に阻止する手段を備えるものであってもよく、また、認証データ復号化手段は、暗号化された第１の認証データを復号化するために生成するデータおよび第２の認証データが、アクセス手段に供給されることを実質的に阻止する手段を備えるものであってもよい。これにより、固有キーや認証データを復元する過程で生成されるデータも秘匿されるから、データが外部に漏れ、固有キーや認証データが逆算される等の危険も減少する。

【０００９】アクセス手段は、第１の乱数を発生する手段と、記憶手段より第１の配送キー情報を取得し、第１の配送キー情報および第１の乱数に基づいて第１の配送キーを作成する手段と、記憶手段より第２の乱数を取得し、第２の乱数および第１の乱数に基づいて第２の配送キー情報を作成し、第２の配送キー情報を記憶手段に供給する手段とを備え、記憶手段は、第２の乱数および第３の乱数を発生する手段と、第２および第３の乱数に基づいて第１の配送キー情報を作成し、第１の配送キー情報および第２の乱数をアクセス手段に供給する手段と、第３の乱数およびアクセス手段より供給された第２の配送キー情報に基づいて、第１の配送キーと実質的に同一

の第２の配送キーを作成する手段とを備えるものであってもよい。これにより、配送キーも、秘匿性を保ったままアクセス手段から記憶手段に送られるので、配送キーが不正に取得され、アクセス手段と記憶手段との間で交換されるデータが不正に復号化される等の危険も減少する。

【００１０】第１乃至第４のダイジェストは、例えば、アクセス手段が、第４の乱数を発生して記憶手段に供給する手段を備え、第１のダイジェスト作成手段が、第１の認証データと、第４の乱数とを変数とする一方向性関数の値を求めることにより第１のダイジェストを作成する手段を備え、第２のダイジェスト作成手段が、第１の認証データと、第３の乱数とを変数とする一方向性関数の値を求めることにより第２のダイジェストを作成する手段を備え、第３のダイジェスト作成手段が、第２の認証データと、第４の乱数とを変数とする一方向性関数の値を求めることにより第３のダイジェストを作成する手段を備え、第４のダイジェスト作成手段が、第２の認証データと、第３の乱数とを変数とする一方向性関数の値を求めることにより第４のダイジェストを作成する手段を備えることにより生成される。

【００１１】アクセス手段は、操作者の操作に従って供給される、操作者を識別する識別情報を、実質的に逆変換が行えないように変換して操作者を特定する署名情報を作成し、署名情報を記憶手段に供給する手段を備え、記憶手段は、アクセス手段より供給された署名情報を取得する手段と、記憶領域に署名情報が記憶されているか否かを判別し、記憶されていないと判別されたとき、アクセス手段より供給された署名情報を記憶領域に記憶し、記憶されていると判別されたとき、記憶されている署名情報と、アクセス手段より供給された署名情報とが、実質的に同一の操作者を示すか否かを判別して、示さないと判別されたとき、アクセス手段が行う指示に従うことを拒絶する手段とを備えるものであってもよい。これにより、既にデータ格納手段の記憶領域にアクセスした者がいる場合、その者以外の者が記憶領域にアクセスすることは実質的に阻止されるので、記憶領域にあるデータが他の者に取得される危険が減少する。

【００１２】

【発明が解決しようとする課題】しかしながら、従来技術には、一台の装置で複数の人がさわることが可能な環境でプライベートなプログラムあるいはデータを鍵情報を基にして各個人が独立して使用することが難しいため、個人で管理するプログラムあるいはデータを他人に使用あるいは引用されることを防ぐことができないという問題点があった。

【００１３】本発明は斯かる問題点を鑑みてなされたものであり、その目的とするところは、一台の装置で複数の人がさわることが可能な環境でプライベートなプログラムあるいはデータを鍵情報を基にして各個人が独立して使用し、個人で管理するプログラムあるいはデータを他人に使用あるいは引用されることを防ぐことができる情報処理装置および私情報セキュリティ方法を提供する点にある。

【００１４】

【課題を解決するための手段】請求項１に記載の発明の要旨は、プログラム格納領域と鍵情報格納領域を備え着脱自在な複数の半導体記憶部と、前記複数の半導体記憶部のうちでどれか一つを選択してシステムバスに接続するセレクタと、外部より鍵情報を入力可能とする鍵情報入力手段と、前記セレクタでどの前記半導体記憶部を選択するかの判断を行うセレクタ判定回路を有し、前記セレクタ判定回路は、前記半導体記憶部の前記鍵情報格納領域に入っている鍵情報と前記鍵情報入力手段から入力された鍵情報とを比較して一致したものの前記半導体記憶部を前記セレクタに選択させる機能を有することを特徴とする情報処理装置に存する。また、請求項２に記載の発明の要旨は、前記複数の半導体記憶部のそれぞれは所定のバスに接続され、前記バスは前記セレクタによって選択的に前記システムバスに接続され、前記システムバスにはブートローダー、プログラム格納領域、主記憶部、ＣＰＵを含む制御回路、前記セレクタ判定回路がそれぞれ接続され、前記鍵情報入力手段は、外部から鍵情報を取得する機能を有し、前記セレクタ判定回路に接続し鍵情報を前記セレクタ判定回路に伝達し、前記セレクタ判定回路は前記セレクタに接続し前記バスのいずれかを前記システムバスに接続するよう前記セレクタに指示を出すように構成されていることを特徴とする請求項１に記載の情報処理装置に存する。また、請求項３に記載の発明の要旨は、前記セレクタは前記複数の半導体記憶部のそれぞれの鍵情報を取得し前記セレクタ判定回路に伝達する手段を有することを特徴とする請求項２に記載の情報処理装置に存する。また、請求項４に記載の発明の要旨は、前記半導体記憶部がＩＣカードにより構成されていることを特徴とする請求項１乃至３のいずれか一項に記載の情報処理装置に存する。また、請求項５に記載の発明の要旨は、前記ＩＣカードを装置にセットして鍵情報を外から与えることにより、個人所有のプログラムを実行させ、プライベートなデータを使って処理を行うことを特徴とする請求項４に記載の情報処理装置に存する。また、請求項６に記載の発明の要旨は、プログラム格納領域と鍵情報格納領域を備え着脱自在な複数の半導体記憶部と、前記複数の半導体記憶部のうちでどれか一つを選択してシステムバスに接続するセレクタと、外部より鍵情報を入力可能とする鍵情報入力手段と、前記セレクタでどの前記半導体記憶部を選択するかの判断を行うセレクタ判定回路を有し、前記セレクタ判定回路は、前記半導体記憶部の前記鍵情報格納領域に入っている鍵情報と前記鍵情報入力手段から入力された鍵情報とを比較して一致したものの前記半導体記憶部を前記セレ

クタに選択させる機能を有する情報処理装置において、前記複数の半導体記憶部のそれぞれの前記鍵情報格納領域にそれぞれ異なる特定の鍵情報を記憶する工程と、前記セレクタが前記鍵情報をバスを通して認識する工程と、前記セレクタ判定回路が前記セレクタに要求を出して前記半導体記憶部に記憶されている各鍵情報を収集する工程と、前記鍵情報入力手段が外部から鍵情報を取得する工程と、前記鍵情報入力手段で入手した鍵情報を前記セレクタ判定回路に送る工程と、前記半導体記憶部の鍵情報と前記鍵情報入力手段から取得した鍵情報が一致したと前記セレクタ判定回路が認識した場合に、前記セレクタを制御して前記バスを前記システムバスに接続するとともに、前記セレクタが当該バスを前記システムバスに接続したことを前記制御回路に通知し、前記セレクタからの通知を基に前記制御回路が、ブートローダーを起動して前記半導体記憶部のプログラム格納領域からプログラムを、前記システムバスに接続している前記プログラム格納領域に転送する工程と、当該転送されたプログラムを前記制御回路のＣＰＵを用いて実行する工程と、新たに前記鍵情報入力手段から取得した鍵情報を基に、前記セレクタ判定回路は前記システムバスを通して前記制御回路に割り込み、実行中のプログラムを停止する工程を有することを特徴とする私情報セキュリティ方法に存する。

【００１５】

【発明の実施の形態】（第１の実施の形態）図１は、本発明の一実施の形態に係る情報処理装置１０を説明するための機能ブロック図である。図１において、１，２，３は半導体記憶部、１Ａ，２Ａ，３Ａはプログラム格納領域、１Ｂ，２Ｂ，３Ｂは鍵情報格納領域、１０は情報処理装置、１２は鍵情報入力手段、１４はセレクタ判定回路、１６は制御回路、１８はセレクタ、２０はブートローダー、２２はプログラム格納領域、２４は主記憶部、２６はシステムバス、３１，３２，３３はバスを示している。

【００１６】本実施の形態の情報処理装置１０は、プログラム格納領域１Ａと鍵情報格納領域１Ｂを備え着脱自在な半導体記憶部１と、プログラム格納領域２Ａと鍵情報格納領域２Ｂを備え着脱自在な複数の半導体記憶部２と、プログラム格納領域３Ａと鍵情報格納領域３Ｂを備え着脱自在な複数の半導体記憶部３と、各半導体記憶部１，２，３のうちでどれか一つを選択してシステムバス２６に接続するセレクタ１８と、外部より鍵情報を入力可能とする鍵情報入力手段１２と、セレクタ１８でどの半導体記憶部１，２，３を選択するかの判断を行うセレクタ判定回路１４を有し、セレクタ判定回路１４は、半導体記憶部１，２，３の鍵情報格納領域１Ｂ，２Ｂ，３Ｂに入っている鍵情報と鍵情報入力手段１２から入力された鍵情報とを比較して一致した半導体記憶部１，２，３をセレクタ１８に選択させる機能を有する点に特徴を有している。

【００１７】半導体記憶部１，２，３はそれぞれバス３１，３２，３３に接続している。バス３１，３２，３３はセレクタ１８によって選択的にシステムバス２６に接続される。

【００１８】システムバス２６にはブートローダー２０、プログラム格納領域２２、主記憶部２４、ＣＰＵを含む制御回路１６、セレクタ判定回路１４がそれぞれ接続されている。

【００１９】鍵情報入力手段１２は、外部から鍵情報を取得する機能を有し、セレクタ判定回路１４に接続し鍵情報をセレクタ判定回路１４に伝達する。

【００２０】セレクタ判定回路１４はセレクタ１８に接続しバス３１，３２，３３のいずれかをシステムバス２６に接続するようセレクタ１８に指示を出す。

【００２１】また、セレクタ１８は半導体記憶部１，２，３の鍵情報を取得しセレクタ判定回路１４に伝達する手段を有する。

【００２２】次に情報処理装置１０の動作（私情報セキュリティ方法）について説明する。図１を参照すると、本実施の形態においては、複数の半導体記憶部１，２，３の鍵情報格納領域１Ｂ，２Ｂ，３Ｂにはそれぞれ異なる特定の鍵情報が記憶されている。

【００２３】セレクタ１８は、この鍵情報をバス３１，３２，３３を通して認識することができる。セレクタ判定回路１４は、セレクタ１８に要求を出して半導体記憶部１，２，３に記憶されている各鍵情報を収集する。

【００２４】鍵情報入力手段１２は外部から鍵情報を取得する手段を有する。例えば、使用者がキーボードよりパスワードを入力したり、スキャナーより指紋情報を入力することも含まれる。鍵の概念は掌紋情報や虹彩情報やその他、多岐にわたるが、ここでは、鍵情報としてパスワードを想定している。すなわち、鍵をパスワードと読み替えてもよい。鍵情報入力手段１２で入手した鍵情報はセレクタ判定回路１４に送られる。

【００２５】ここで、半導体記憶部１の鍵情報と鍵情報入力手段１２から取得した鍵情報が一致したとセレクタ判定回路１４が認識した場合、セレクタ１８を制御してバス３１をシステムバス２６に接続する。セレクタ１８はバス３１をシステムバス２６に接続したことを制御回路１６に通知する。この通知はバス３１に限らず、バス３２，３３のうちいずれかがシステムバス２６に接続されていれば、セレクタ１８は制御回路１６に通知を行う。

【００２６】制御回路１６は、セレクタ１８からの通知を基に、ブートローダー２０を起動して半導体記憶部１のプログラム格納領域１Ａからプログラムを、システムバス２６に接続しているプログラム格納領域２２に転送する。そして転送されたプログラムを制御回路１６のＣＰＵを用いて実行する。

【００２７】新たに鍵情報入力手段１２から取得した鍵情報を基に、セレクタ判定回路１４はシステムバス２６を通して制御回路１６に割り込み、実行中のプログラムを停止する。

【００２８】なお、本実施の形態では、半導体記憶部１，２，３が３つの例を示したが、これに特に限定されることなく、１つから有限のｎ（自然数）個までの拡張を考えることは容易である。

【００２９】本実施の形態は以上のように構成されているので、以下に掲げる効果を奏する。まず第１の効果は、鍵情報を入力させ、それに対応する半導体記憶部１，２，３のプログラムを実行させることができることから、鍵を保有する人それぞれの必要とするプログラムやデータを使って動作させることができることである。

【００３０】また第２の効果は、他の人には実行させることができないことから、間違えや明らかな故意によりプログラムやデータを用いることを禁止することができることである。

【００３１】また第３の効果は、複数の半導体記憶部１，２，３を接続できることにより必要なプログラムを選択的に選ぶことができることである。例えば、本情報処理装置１０がテレビゲームとして用いられることを想定した場合には使用者が必要なプログラム（ゲーム）を選択して使用できるようになるといった効果を奏する。

【００３２】そして第４の効果は、半導体記憶部１，２，３を取り付け、取り外し可能とすることによりプログラムの変更または拡張が容易に実行できることである。例えば、半導体記憶部１，２，３にプログラムと同時にディジタルカメラのデータや音楽のディジタルデータを入れてある場合に、必要に応じて容易にデータの交換ができるようになるといった効果を奏する。

【００３３】（第２の実施の形態）本実施の形態は、半導体記憶部１，２，３がＩＣカードにより構成され、情報処理装置１０にセットして鍵情報を外から与えることにより、個人所有のプログラムを実行させ、プライベートなデータを使って処理を行う点に特徴を有している。

【００３４】なお、本発明が上記各実施の形態に限定されず、本発明の技術思想の範囲内において、各実施の形態は適宜変更され得ることは明らかである。また上記構成部材の数、位置、形状等は上記実施の形態に限定されず、本発明を実施する上で好適な数、位置、形状等にすることができる。また、各図において、同一構成要素には同一符号を付している。

【００３５】

【発明の効果】本発明は以上のように構成されているので、以下に掲げる効果を奏する。まず第１の効果は、鍵情報を入力させ、それに対応する半導体記憶部のプログラムを実行させることができることから、鍵を保有する人それぞれの必要とするプログラムやデータを使って動作させることができることである。

【００３６】また第２の効果は、他の人には実行させることができないことから、間違えや明らかな故意によりプログラムやデータを用いることを禁止することができることである。

【００３７】また第３の効果は、複数の半導体記憶部を接続できることにより必要なプログラムを選択的に選ぶことができることである。例えば、本情報処理装置がテレビゲームとして用いられることを想定した場合には使用者が必要なプログラム（ゲーム）を選択して使用できるようになるといった効果を奏する。

【００３８】そして第４の効果は、半導体記憶部を取り付け、取り外し可能とすることによりプログラムの変更または拡張が容易に実行できることである。例えば、半導体記憶部にプログラムと同時にディジタルカメラのデータや音楽のディジタルデータを入れてある場合に、必要に応じて容易にデータの交換ができるようになるといった効果を奏する。

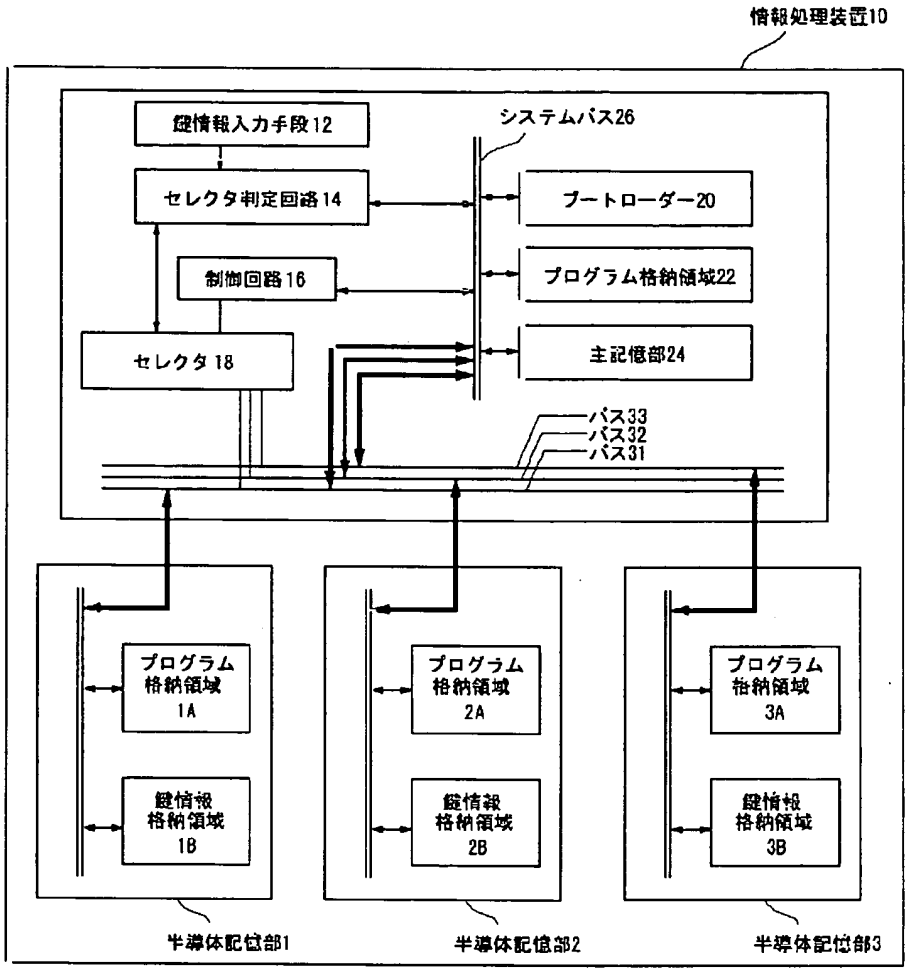
【図面の簡単な説明】

【図１】本発明の一実施の形態に係る情報処理装置を説明するための機能ブロック図である。

【符号の説明】

１，２，３…半導体記憶部
１Ａ，２Ａ，３Ａ…プログラム格納領域
１Ｂ，２Ｂ，３Ｂ…鍵情報格納領域
１０…情報処理装置
１２…鍵情報入力手段
１４…セレクタ判定回路
１６…制御回路
１８…セレクタ
２０…ブートローダー
２２…プログラム格納領域
２４…主記憶部
２６…システムバス
３１，３２，３３…バス

【図1】


情報処理装置10
鍵情報入力手段12
システムバス26
セレクタ判定回路14
ブートローダー20
制御回路16
プログラム格納領域22
セレクタ18
主記憶部24
バス33
バス32
バス31
プログラム格納領域 1A
鍵情報格納領域 1B
プログラム格納領域 2A
鍵情報格納領域 2B
プログラム格納領域 3A
鍵情報格納領域 3B
半導体記憶部1
半導体記憶部2
半導体記憶部3